Redacted Version

SEALED BY ORDER OF THE COURT

FILED
Sep 07 2021
SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

FILED
SEP 07 2022
CLERK, U.S. DISTRICT COURT
NORTH DISTRICT OF CALIFORNIA
SAN JOSE OFFICE

UNITED STATES DISTRICT COURT

for the

Northern District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Three Electronic Devices for Apprehension of Persons to be Arrested

Case No. CR 21-71420-NC

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of New Jersey , there is now concealed *(identify the person or describe the property to be seized):*

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more):*

- ☐ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Fed. R. Crim. P. 41(c)	Apprehension of Person to be Arrested Pursuant to Previously Issued Warrant
21 U.S.C. § 841(a)(1)	Possession with intent to distribute and distribution of methamphetamine
18 U.S.C. § 922(g)(1)	Felon in possession of a firearm/ammunition

The application is based on these facts:

See affidavit of FBI Special Agent Meagan Sharp

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 30 days *(give exact ending date if more than 30 days: _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

CERTIFICATION: I am an attorney for the government. Applicant's agency is conducting an ongoing criminal investigation, and the information likely to be obtained through this application is relevant to that investigation. */s/ Christoffer Lee*
AUSA Christoffer Lee

/S/
Applicant's signature
Meagan Sharp, FBI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by _____ *(specify reliable electronic means).*

Date: 9/3/2021

Judge's signature

City and state: San Jose, CA

Hon. Nathanael Cousins, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANT

I, Meagan Sharp, a Special Agent of the Federal Bureau of Investigation (the "FBI"), being duly sworn, hereby declare as follows:

PURPOSE OF AFFIDAVIT

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c)(1)(A) for subscriber information, as well as historical and prospective location information associated with the following cellular telephones ("**TARGET TELEPHONES**"):

a. Phone Number: **(408) 621-[redacted]** (hereinafter **"Target Cell Phone 1"**)
Service Provider: AT&T[1]
Subscriber: Ramiro Velasco
Subscriber Address: [redacted], Visalia, CA 93291
Suspected User: RAMIRO VELASCO aka, "Rome"

b. Phone Number: **(559) 740-[redacted]** (hereinafter **"Target Cell Phone 2"**)
Service Provider: AT&T
Subscriber: Prepaid User
Subscriber Address: 123 Your Street, Your Town, GA 93277[2]
Suspected User: DEREK WILLIAMS, aka "Baby D"

c. Phone Number: **(510) 346-[redacted]** (hereinafter **"Target Cell Phone 3"**)
Service Provider: T-Mobile[3]
Subscriber: [redacted]
Subscriber Address: [redacted], San Jose, CA 95111
Suspected User: FELIPE MUNOZ, aka "Shark"

d. Phone Number: **(669) 300-[redacted]** (hereinafter **"Target Cell Phone 4"**)
Service Provider: Verizon Wireless[4]
Subscriber: Evan Kobayashi
Subscriber Address: [redacted], San Jose, CA 95133
Suspected User: EVAN KOBAYASHI, aka "Evan Eyes"

[1] AT&T is a wireless cellular telephone service provider headquartered at 11760 Us Hwy 1, North Palm Beach, Florida 33408.
[2] The address provided by AT&T when subpoenaed for telephone subscriber information.
[3] T-Mobile USA is a wireless cellular telephone service provider headquartered at 4 Sylvan Way, Parsippany, New Jersey 07054.
[4] Verizon Wireless is a wireless cellular telephone service provider headquartered at 170 Washington Valley Road, Bedminster, NJ 07921.

e. Phone Number: **(408) 841-[redacted]** (hereinafter "**Target Cell Phone 5**")
Service Provider: T-Mobile
Subscriber: [redacted]
Subscriber Address: [redacted], San Jose, CA 95110
Suspected User: MARCO URBINA

2. The **TARGET TELEPHONES** are described herein and in Attachment A, and the information to be seized is described herein and in Attachment B.

3. This application seeks a warrant directing AT&T, T-Mobile USA, and Verizon Wireless to provide subscriber information, historical phone tolls with cell site data from August 15, 2021 until the date the warrant issues, and to provide 30 days of prospective location information from the date the warrant issues. The suspected users of the **TARGET TELEPHONES**—RAMIRO VELASCO, DEREK WILLIAMS, FELIPE MUNOZ, EVAN KOBAYASHI, and MARCO URBINO (the **TARGET PERSONS**)—were indicted for violations of 21 U.S.C. § 841(a)(1) and/or 18 U.S.C. § 922(g)(1) on September 1, 2021. *See* United States District Court for the Northern District of California Case Nos. 21-cr-342 LHK (VELASCO and WILLIAMS), 21-cr-345 BLF (MUNOZ), 21-cr-344 BLF (KOBAYASHI), and 21-cr-347 LHK (URBINA). United States Magistrate Judge Sallie Kim issued no bail arrest warrants for the **TARGET PERSONS.** Thus, the **TARGET PERSONS** are persons to be arrested within the meaning of Rule 41(c)(4) of the Federal Rules of Criminal Procedure.

4. As described below, previous attempts to determine the locations of the **TARGET PERSONS** have been unsuccessful.

5. Because this warrant seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a "pen register" and/or "trap and trace device," *see* 18 U.S.C. § 3127(3) & (4), the requested warrant is designed to also comply with the Pen Register Act. *See* 18 U.S.C. §§ 3121-3127. The requested warrant therefore includes all the information required to be included in an order pursuant to that statute. *See* 18 U.S.C. § 3123(b)(1).

6. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that the **TARGET PERSONS** are users of the **TARGET**

TELEPHONES, described in Attachment A. Further, there is probable cause to believe that the information sought in Attachment B—subscriber information, historical location information, and prospective location information—will assist law enforcement in determining the location of the **TARGET PERSONS**, who are persons to be arrested within the meaning of Rule 41(c)(4) of the Federal Rules of Criminal Procedure.

7. The facts in this affidavit come from my personal observations, my training and experience, information from records and databases, and information obtained from other agents/officers and witnesses. This affidavit does not set forth all of my knowledge about this matter; it is intended only to show that there is sufficient probable cause for the requested warrant. My understanding of the facts and circumstances may evolve as the investigation progresses.

AFFIANT BACKGROUND

8. I am a Special Agent with the Federal Bureau of Investigation and have been since July 2018. As an FBI agent, I am authorized to investigate violations of United States law and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States. I am currently assigned to the San Jose Violent Crime Unit of the FBI's San Francisco Field Division. Prior to becoming an FBI Special Agent, I was an Analyst for the Department of Defense. Before becoming an FBI Special Agent, I completed the five-month FBI Special Agent Basic Training program at the FBI academy in Quantico, Virginia.

9. As an FBI Special Agent, I investigate individuals who are involved in the illegal possession and transfer of firearms, violent crimes involving firearms, and narcotics trafficking. During the course of my employment with the FBI, I have investigated, and also assisted in the investigation of, criminal violations relating to firearms and/or narcotics. During these investigations, I have participated in and utilized the following investigative tools: conducting physical surveillance, interviewing suspects, writing affidavits for search warrants, executing arrest and search warrants, analyzing phone records obtained from pen registers, trap and trace devices, and physical devices, collecting and processing evidence, and reviewing search warrant

results from social media accounts. In addition, I have received specialized training in the extraction of data from digital devices, including cellular telephones. I also have received training specific to investigations that focused on topics such as money-laundering techniques and schemes, drug trafficking organizations, and successful management of confidential human sources.

10. Through my training and experience, I have become familiar with the methods and means used by gang members, street gangs, and their associates to conduct illegal activity. I have interviewed gang members and associates regarding gang activity, as well as reviewed recorded communications between active gang members and associates. As such, I have become knowledgeable about the criminal activities committed by gang members in the San Francisco Bay area and the purposes and underlying reasons for the commission of such criminal activities. I also have become familiar with the ways in which gang members show their affiliation and interact with each other and rival gang members. As such, I have become familiar with the methods used by gang members and their associates to commit crimes, conceal evidence of their crime(s), and to prevent witnesses from cooperating with law enforcement, or testifying for the government.

11. Based on my training and experience, I know that gang members (including those who distribute narcotics), drug traffickers, and their associates often use cellular telephones in order to communicate about gang activity, crimes, illegal narcotics distribution, and the acquisition/possession of handguns, rifles, assault rifles and ammunition. Such communications include phone calls, text- and media-messages, app-based communications, and emails. Communication devices such as cellular telephones are used to coordinate with other co-conspirators regarding location, pricing, and to provide/receive other information in order to further facilitate this criminal activity.

12. In addition, I know that such persons typically maintain consistent possession of and travel with their cellular telephones. This constant possession of cellular telephones may facilitate communication concerning both legal and illegal activity, but aids in the ability of law

enforcement to seek location information concerning the user of such cell phones. Therefore, the location data of the cellular telephone assists investigators in determining patterns of travel, identifying those who may be associating with one another, as well as locating potential co-conspirators, places in which illicit activity is conducted (including drug sales and other gang-related activity), locations in which contraband is stored, and the whereabouts of persons to be arrested.

13. Based on my training, experience and knowledge of this investigation, I know gang members and drug dealers often register telephones in the name of family members, friends, girlfriends, wives, fictitious names, or even no names at all, in order to hide their criminal activity from law enforcement and the true identity of the actual user of the phone. They will often have more than one phone in order to conduct criminal activity on one and the second number for family friends and to show law enforcement.

14. I have been involved in the execution of search warrants of premises as well as cellular accounts/devices, including: residences, telephones and other electronic devices, telephone service providers for location information, and social media accounts.

15. I am an investigator and law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7). I am empowered by law to conduct investigations, to execute search warrants, and to make arrests for offenses of Federal law

APPLICABLE STATUTES

16. This investigation concerns the following violations of federal law—21 U.S.C. § 841(a)(1), (b)(1)(B)(viii) possession with intent to distribute and distribution of methamphetamine and 18 U.S.C. § 922(g)(1) felon in possession of a firearm/ammunition— as alleged in the indictments issued in Northern District of California Case Nos. 21-cr-342 LHK (VELASCO and WILLIAMS), 21-cr-345 BLF (MUNOZ), 21-cr-344 BLF (KOBAYASHI), and 21-cr-347 LHK (URBINA), otherwise referred to as the ("**Target Offenses**").

17. The **TARGET PERSONS** are persons to be arrested within the meaning of Rule 41(c)(4) of the Federal Rules of Criminal Procedure, given the arrest warrants issued by the

Honorable Sallie Kim, United States Magistrate Judge for the United States District Court, for the Northern District of California, on September 1, 2021.

18. **Jurisdiction.** The court has jurisdiction to issue the proposed warrant because it is a "court of competent jurisdiction" as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i) and/or is in a district in which the items described in Attachment A are stored, *see* 18 U.S.C. § 2711(3)(A)(ii).

19. **Stored Wire and Electronic Communication Access.** Title 18, United States Code, Chapter 121, Sections 2701 through 2711, is entitled "Stored Wire and Electronic Communications and Transactional Records Access." The government may obtain records and other information pertaining to a subscriber or customer of electronic communication service or remote computing service by way of a search warrant. *See* 18 U.S.C. § 2703(c)(1)(A).

STATEMENT OF PROBABLE CAUSE

A. Introduction and Factual Summary

20. A grand jury sitting for the Northern District of California returned indictments on September 1, 2021 charging the **TARGET PERSONS** with violations of 21 U.S.C. § 841(a)(1), (b)(1)(B)(viii) (VELASCO, WILLIAMS, MUNOZ, and KOBAYASHI) and 18 U.S.C. § 922(g)(1) (MUNOZ and URBINA). The Honorable Sallie Kim, United States Magistrate Judge, issued warrants for each **TARGET PERSON**'s arrest. The indictments and warrants remain under seal.

21. The instant application for a search warrant seeks subscriber information, as well as historical and prospective location information, for the **TARGET TELEPHONES**, as described with more particularity in Attachment A, so as to assist in apprehending the **TARGET PERSONS** on their federal arrest warrants.

22. The following paragraphs set forth the probable cause for believing that each **TARGET TELEPHONE** is associated with each **TARGET PERSON**, and previous, unsuccessful efforts to locate each TARGET PERSON through other means.

TARGET: RAMIRO VELASCO Target Cell Phone 1 (408) 621-[redacted]

23. VELASCO contacted an FBI Confidential Human Source (CHS-1)[5] in October 2020 from telephone number (408) 621-[redacted] (**Target Cell Phone 1**) to facilitate a narcotics

[redacted]

5 [redacted]

purchase. [redacted].

24. After a second controlled narcotics purchase with VELASCO's source of supply, CHS-1 received a call from VELASCO on **Target Cell Phone 1**. During the phone call, VELASCO told CHS-1 he was in San Jose and they should meet up. [redacted] Thus, Velasco used **Target Cell Phone 1** to facilitate a narcotics purchase.

25. [redacted], at the direction of law enforcement, CHS-1 attended gang meeting for SJG. This [redacted] SJG meeting occurred at the residence of SJG member [redacted], CHS-1 subsequently debriefed law enforcement, advised that VELASCO was present at the meeting, and indicated VELASCO is still using **Target Cell Phone 1**.

26. On July 23, 2021, law enforcement served AT&T with an Administrative Subpoena requesting subscriber information and toll records for **Target Cell Phone 1**. Results of the subpoena indicated **Target Cell Phone 1** was subscribed to "Ramiro Velasco, [redacted], Visalia, CA 93291." The telephone number has been in use since May 10, 2020, with no breaks in service.

27. Law enforcement previously surveilled two addresses associated with VELASCO or family members of VELASCO and did not observe VELASCO at either location. Law enforcement believes VELASCO may also stay in Visalia, CA. Due to multiple associated addresses, law enforcement has been unable to locate VELASCO. The requested ping warrant and historical data should assist law enforcement in determining VELASCO's patterns of movements and current location to facilitate service of his arrest warrant.

TARGET: DEREK WILLIAMS Target Cell Phone 2 (559) 740-[redacted]

28. WILLIAMS was released on parole in Visalia, CA on August 2, 2020. On August 17, 2021, WILLIAMS contacted his parole officer using telephone number (559) 740-[redacted] (**Target Cell Phone 2**). On August 18, 2021, law enforcement served AT&T with an Administrative Subpoena requesting subscriber information and toll records for **Target Cell Phone 2**. Results of the subpoena indicate **Target Cell Phone 2** was a Prepaid Customer and has been active since July 2, 2021.

29. An analysis of toll records received from AT&T for **Target Cell Phone 2** from approximately July 1, 2021 to August 17, 2021 also revealed multiple communications between **Target Cell Phone 2** (WILLIAMS) with **Target Cell Phone 1** (VELASCO). VELASCO and WILLIAMS are co-defendants in Northern District of California Case Nos. 21-cr-342 LHK (charging each with violations of 18 U.S.C. § 841(a)(1)).

30. From the time WILLAMS was released from prison, and more specifically in the last three months, WILLIAMS has provided parole multiple addresses and has been non-responsive to parole phone calls. Law enforcement has been unable to locate WILLIAMS. On December 21, 2020, WILLIAMS reported to parole he was still homeless and had been staying in various places in Visalia, CA. On July 23, 2021, parole documented that WILLIAM's performance on parole was "extremely poor" and he has an unstable residential pattern. Parole agents report that WILLIAMS has absconded from parole and parole does not know his current residence. The requested ping warrant and historical data should assist law enforcement in determining WILLIAMS' patterns of movements and current location to facilitate service of his arrest warrant.

TARGET: FELIPE MUNOZ Target Cell Phone 3 (510) 346-[redacted]

31. MUNOZ is currently on pre-trial supervision in Santa Clara County based on criminal cases in Santa Clara County Superior Court. On or around August 4, 2021, Santa Clara County pre-trial services provided the phone number of (510) 346-[redacted] (**Target Cell Phone 3**)

as MUNOZ's current number and [redacted], San Jose, CA 95124 as MUNOZ's address.

32. On August 5, 2021, law enforcement served T-Mobile with an Administrative Subpoenas requesting subscriber information and toll records for **Target Cell Phone 3**. Results of the subpoena indicate **Target Cell Phone 3**, is subscribed to [redacted], San Jose, CA 95111." A query of the DMV data base indicates MUNOZ's listed address on his California Driver's License is [redacted], San Jose, CA 95111, the same address as the subscriber for **Target Cell Phone 3**. Additionally, I know MUNOZ is currently on probation in Santa Clara County as well, and his listed address with Santa Clara County Probation is also [redacted], San Jose, CA 95111.

33. An analysis of toll records received from T-Mobile for **Target Cell Phone 3** from approximately June 1, 2021 to August 3, 2021 reveal **Target Cell Phone 3** is in use. Law enforcement identified 14 call events with [redacted] between July 21, 2021 and July 22, 2021. Law enforcement databases identified [redacted] as associated to [redacted], a known SJG gang associate. MUNOZ and [redacted]

34. Law enforcement previously surveilled and conducted a ruse operation at [redacted], San Jose, CA 95124 to attempt to identify MUNOZ at the residence. On August 6, 2021, a female answered the door and when asked if MUNOZ was there the female stated he was downstairs. Due to MUNOZ's recent release, it was believed MUNOZ possibly lived in a vehicle parked in a parking spot associated with [redacted] San Jose, CA 95124. However, to date, law enforcement has not identified MUNOZ at the residence. MUNOZ has provided probation and pre-trial services different addresses and law enforcement has been unable to locate MUNOZ since his pre-release on August 4, 2021 on pending state charges. The requested ping warrant and historical data should assist law enforcement in

determining MUNOZ's patterns of movements and current location to facilitate service of his arrest warrant.

TARGET: EVAN KOBAYASHI Target Cell Phone 4 (669) 300-[redacted]

35. On August 5, 2021, law enforcement served Verizon Wireless with an Administrative Subpoena requesting subscriber information and toll records for **Target Cell Phone 4**. Results of the subpoena indicate **Target Cell Phone 4** was subscribed to EVAN KOBAYASHI, [redacted], San Jose, CA 95133. The telephone number has been in use since May 25, 2020. I know KOBAYASHI is currently on probation and his address on record is [redacted], San Jose, CA 95133, the same as subscriber information for **Target Cell Phone 4**.

36. An analysis of toll records received from Verizon Wireless for **Target Cell Phone 4** from approximately May 15, 2020 to August 3, 2021 revealed numerous call events between known SJG members and associates.

37. On July 13, 2021, law enforcement conducted surveillance on KOBAYASHI and followed him to [redacted], San Jose, CA where he remained for the duration of the surveillance. However, law enforcement has learned that, at times, KOBAYASHI has been homeless. Multiple attempts to surveil KOBAYASHI at [redacted], San Jose, CA since July 13, 2021 have failed to place him at that location. The requested ping warrant and historical data should assist law enforcement in determining KOBAYASHI's patterns of movements and current location to facilitate service of his arrest warrant.

TARGET: MARCO URBINA Target Cell Phone 5 (408) 841-[redacted]

38. On May 12, 2021, San Jose Police Department (SJPD) executed a search warrant on [redacted] San Jose, CA, a residence associated with URBINA. During surveillance operations prior to the search, SJPD observed URBINA and others involved with actions consistent with those of illegal narcotics sales, to include hand-to-hand transactions with multiple subjects and evasive driving to and from the meet locations. SJPD arrested URBINA after the search warrant execution.

39. On August 30, 2021, URBINA called SJPD Property and Evidence from (408) 841-[redacted] (**Target Cell Phone 5**) to retrieve his possessions from the above arrest. URBINA told SJPD **Target Cell Phone 5** was his number and the best way to reach him.

40. On August 31, 2021, law enforcement served T-Mobile with an Administrative Subpoena requesting subscriber information and toll records for **Target Cell Phone 5**. Results of the subpoena indicate **Target Cell Phone 5** is subscribed to [redacted], San Jose, CA 95110, and has been active since February 25, 2021.

41. Based on my training and experience, I know that criminals tend to register cell phone numbers under an alias or another person's name to evade law enforcement and disguise their illicit activities.

42. An analysis of toll records received from T-Mobile for **Target Cell Phone 5** from approximately May 1, 2021 to August 30, 2021 reveal that **Target Cell Phone 5** had 555 call events with (408) 991-[redacted] a known number associated to URBINA's [redacted] and between May 1, 2021 and August 1, 2021, **Target Cell Phone 5** had 27 call events with (408) 841-[redacted] a known number associated to URBINA's brother, Max Urbina, a known SJG gang associate. Marco URBINA and Max Urbina are co- defendants in Northern District of California Case No. 21-cr-347), which alleges violations of 18 U.S.C. § 922(g)(1).

43. URBINA has been associated to multiple addresses in the San Jose area and law enforcement has identified vehicles registered to and driven by URBINA located at multiple residences. On August 25, 2021, law enforcement observed URBINA get dropped off at [redacted], San Jose, CA (a known address), but URBINA entered another vehicle and departed the location. URBINA has not been located since. The requested ping warrant and historical data should assist law enforcement in determining URBINA's patterns of movements and current location to facilitate service of his arrest warrant.

44. Based on the foregoing and my training and experience, there is probable cause to believe that the requested subscriber information, historical location data, and prospective location monitoring sought in Attachment B will help to assist law enforcement to confirm the

TARGET PERSONS' residence(s) and establish patterns of movement, facilitate surveillance, and aid law enforcement in apprehending each on his federal warrant.

45. Based on my training and experience, many people carry a cell phone with them at most times. As described below, the cell phone's communications with the cell phone provider's tower may be captured by the provider and a review of that data can be used to locate the user of the cell phone.

B. Training and Experience Regarding Cellular Telephones and Provider Technology and Information

46. Based on my training and experience, I have learned that AT&T, Verizon Wireless, T-Mobile USA are each a company that provides cellular telephone access to the general public.

47. **Subscriber Information.** In my training and experience, I have learned that wireless providers maintain business records and subscriber information for particular accounts. This information could include the subscribers' full names, user names, mailing and e-mail addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service utilized, the Electronic Serial Number ("ESN") or other unique identifier for the cellular device associated with the account, the subscribers' Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates and times of payments and the means and source of payment (including any credit card or bank account number). In some cases, wireless subscribers may communicate directly with a wireless provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Wireless providers typically retain records about such communications, including records

of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

48. **Other Records**. In my training and experience, I have learned that wireless providers also maintain other records associated with each particular cellular device. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an ESN, a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Station Equipment Identity ("IMEI").

49. Wireless phone providers typically retain certain transactional information about the use of each telephone, voicemail, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers or e-mail addresses associated with particular telephone calls, voicemail messages, and text or multimedia messages. Providers may also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved.

50. Wireless phone providers commonly provide customers internet connectivity and retain certain transactional information about internet activity. This information can include the Internet protocol ("IP") address used by the phone and logs showing all internet activity on the account (namely sites visited by a user, records of internet session dates and times, and other information).

51. **Location Data.** In my training and experience, I know that when a cellular device connects to a cellular antenna or tower ("cell towers" or antenna towers covering specific geographic areas), it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of

course. Many wireless providers retain information about the location in which a particular communication was transmitted or received. This information can include data about which cell towers received a radio signal from the cellular device and thereby transmitted or received the communication in question.

52. In my training and experience, I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including E-911 Phase II data, also known as GPS data or latitude-longitude data, and cell-site data, also known as "tower/face information" or cell tower/sector records. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise than E-911 Phase II data. With respect to both E-911 Phase II data and cell site data, the service provider accesses location data that already exists on the device and then processes that data (sometimes with other information such as signal measurements from cell towers) so that it can be used and interpreted.

53. Based on my training and experience, I know that for each communication a cellular device makes, its service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as the service provider typically collect and retain cell-

site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

54. In addition, I am aware that in the ordinary course of their business, providers of cellular telephone service, like AT&T, Verizon Wireless, T-Mobile USA, collect network timing information that may also assist in identifying the approximate location of a handset. I understand that different providers collect this network timing information in different ways and may have different names for it. Some examples of this network timing information include Sprint's Per Call Measurement Data (PCMD), Verizon's Real Time Tool (RTT), AT&T's Network Event Location System (NELS), and T-Mobile's True Call Data.

55. In my training and experience, I know that wireless providers such as AT&T, Verizon Wireless, T-Mobile USA typically collect and retain the above information in their normal course of business. This information (1) can be used to identify and confirm the **TARGET TELEPHONES**'s user or users, (2) historical location data may be used to place the **TARGET TELEPHONES** at or near the **TARGET PERSONS**' prior residences or to establish patterns of movement; and (3) prospective location may be used to locate the **TARGET TELEPHONES** and thus assist in the subsequent apprehension of the **TARGET PERSONS.**

AUTHORIZATION REQUEST

56. Based on the foregoing, there is probable cause to believe that the users of the **TARGET TELEPHONES** are persons to be arrested, within the meaning of Rule 41(c) of the Federal Rules of Criminal Procedure pursuant to their federal arrest warrants. I further believe that the information sought in Attachments A and B will assist law enforcement to confirm the **TARGET PERSONS**' residences, to establish patterns of movement, facilitate surveillance, and to ultimately apprehend the **TARGET PERSONS** on their federal arrest warrants.

57. Accordingly, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c).

58. I further request that the Court direct AT&T, Verizon Wireless, T-Mobile USA to disclose to the government any information described in Attachment B that is within the

possession, custody, or control of AT&T, Verizon Wireless, T-Mobile USA, respectively. I also request that the Court direct AT&T, Verizon Wireless, T-Mobile USA to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with the AT&T, Verizon Wireless, T-Mobile USA services. The government shall reasonably compensate AT&T, Verizon Wireless, T-Mobile USA for reasonable expenses they incur in connection with complying with the Warrant.

59. Because I will submit the warrant to AT&T, Verizon Wireless, T-Mobile USA, I further request that the Court authorize execution of the warrant at any time of day or night, owing to this transmission to AT&T, Verizon Wireless, T-Mobile USA and the potential need to locate the **TARGET TELEPHONES** outside of daytime hours.

REQUEST FOR DELAYED NOTIFICATION AND SEALING

60. The indictments and federal arrest warrants for the **TARGET PERSONS** are under seal. If the **TARGET PERSONS** or anyone associated with each is notified that agents sought or received the requested warrant, the users and their associates are likely to take steps to frustrate the agents' ongoing investigative efforts. Notification at the time of the warrant and order would jeopardize the integrity of this ongoing investigation and would increase the risk that targets of the investigation would flee. I also believe that notifying the target of the investigation would cause the **TARGET PERSONS** to change patterns of activity, flee the jurisdiction, and potentially thwart the efforts of law enforcement to locate them.

61. Accordingly, there is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or

electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

62. I therefore also request, under 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure Rule 41(f)(3), that the Court authorize notice to be delayed for a period of 30 days after the termination of the monitoring period authorized by the warrant, unless further extended by good cause.

63. I further request, in order to avoid compromising this ongoing investigation, to avoid the subjects' flight, and for the safety of the agents and officers, that this application and affidavit, warrant, and order be filed under seal until further order of the Court, except that working copies should be made available to the United States Attorney's Office, the Federal Bureau of Investigation, any other law enforcement agency designated by the United States Attorney's Office, and to AT&T, Verizon Wireless, T-Mobile USA as necessary to effect this Court's order.

I declare under penalty of perjury that the above is true and correct to the best of my knowledge and belief.

Respectfully submitted,

/S/ Phone

Meagan Sharp
Special Agent
Federal Bureau of Investigation

Sworn to ~~before~~ me over the telephone and signed by me pursuant to Fed. R. Crim. P. 4.1 and 4(d) on this 7 day of September, 2021. This application and warrant are to be filed under seal.

HONORABLE NATHANAEL COUSINS
United States Magistrate Judge

ATTACHMENT A

Property to be Searched

1. The cellular telephones described as follows (collectively the "**TARGET TELEPHONES**"):

a. Phone Number: **(408) 621-[redacted]** (hereinafter **"Target Cell Phone 1"**)
Service Provider: AT&T
Subscriber: Ramiro Velasco
Subscriber Address: [redacted] Visalia, CA 93291
Suspected User: RAMIRO VELASCO aka, "Rome"

b. Phone Number: **(559) 740-[redacted]** (hereinafter **"Target Cell Phone 2"**)
Service Provider: AT&T
Subscriber: Prepaid User
Subscriber Address: 123 Your Street, Your Town, GA 93277
Suspected User: DEREK WILLIAMS, aka "Baby D"

c. Phone Number: **(510) 346-[redacted]** (hereinafter **"Target Cell Phone 3"**)
Service Provider: T-Mobile
Subscriber: [redacted]
Subscriber Address: [redacted], San Jose, CA 95111
Suspected User: FELIPE MUNOZ, aka "Shark"

d. Phone Number: **(669) 300-[redacted]** (hereinafter **"Target Cell Phone 4"**)
Service Provider: Verizon Wireless
Subscriber: Evan Kobayashi
Subscriber Address: [redacted], San Jose, CA 95133
Suspected User: EVAN KOBAYASHI, aka "Evan Eyes"

e. Phone Number: **(408) 841-[redacted]** (hereinafter "**Target Cell Phone 5**")
Service Provider: T-Mobile
Subscriber: [redacted]
Subscriber Address: [redacted], San Jose, CA 95110
Suspected User: MARCO URBINA

2. Records and information associated with the **Target Cell Phones 1 and 2** that are within the possession, custody, or control of AT&T Wireless, which is headquartered at 11760 U. S. Hwy 1, N. Palm Beach, Florida 33408.

3. Records and information associated with the **Target Cell Phones 3 and 5** that are within the possession, custody, or control of T-MOBILE USA, which is headquartered at 4 Sylvan Way, Parsippany, NJ 07054.

4. Records and information associated with the **Target Cell Phone 4** that are within the possession, custody, or control of Verizon Wireless, which is headquartered at 170 Washington Valley Road, Bedminster, NJ 07921.

ATTACHMENT B

Particular Things to be Seized

I. Subscriber and Historical Location Information to be Disclosed by the Service Provider (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the **Provider**, and/or stored at its premises, including any information that has been deleted but is still available to the **Provider** or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the **Provider** is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period from August 15, 2021 until 30 days after the date of the warrant:

a. **Subscriber Information.** The following information about the customers or subscribers of the Account:

i. Names (including subscriber names, user names, and screen names);

ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

iii. Local and long-distance telephone connection records;

iv. Call Detail Records to include but not limit to, cell sites, session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses and source port) associated with those sessions, voice, push to talk, non-content text message incoming and outgoing, SMS, MMS, data sessions, PCMD – Per Call Measurement Data, packet data activity records and any other stored records pertaining to packet data transmission, as well as the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers, email addresses, and IP addresses) if not otherwise provided for in the call detail records described above;

v. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

vi. Length of service (including start date) and types of service utilized;

vii. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

viii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

ix. Means and source of payment for such service (including any credit card or bank account number) and billing records.

b. **Historical Location Information.** To the extent not otherwise provided, all historical "location information" related to the **TARGET TELEPHONE**, including:

i. Location information about which "cell towers" (i.e., antenna towers covering specific geographic areas) and "sectors" (i.e., faces of the towers) received a radio signal from (or otherwise communicated with) the **TARGET TELEPHONE** described in Attachment A; and

ii. Location information about the **TARGET TELEPHONE** includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information, as well as all data about which cell towers and sectors received a radio signal from (or otherwise communicated with) the **TARGET TELEPHONE** described in Attachment A.

II. Prospective Location Information to be Disclosed by the Provider

All information about the location of the Target Telephone described in Attachment A for a period of thirty days, during all times of day and night. "Information about the location of the Target Cell Phone" includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information, including records relating to timing data, such as Sprint's Per Call Measurement Data (PCMD), Verizon's Real Time Tool (RTT), AT&T's Network Event Location System (NELS), and T-Mobile's True Call Data, as well as all data about which "cell

towers" (i.e., antenna towers covering specific geographic areas) and "sectors" (i.e., faces of the towers) received a radio signal from the cellular telephone described in Attachment A.

To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of the **Provider**, the **Provider** is required to disclose the Location Information to the government. In complying with this order, the **Provider** is not required to retrieve data that exists on the cellular telephone that is not otherwise in its possession, custody or control.

The government shall compensate the **Provider** for reasonable expenses incurred in disclosing this information.

This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

III. Information to be Seized by the Government

All information described above in Sections I and II that will assist in arresting RAMIRO VELASCO, DEREK WILLIAMS, FELIPE MUNOZ, EVAN KOBAYASHI, and MARCO URBINO, each of whom is the subject of a federal arrest warrant issued on September 1, 2021 by the United States District Court for the Northern District of California and is therefore a "person to be arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.